The Journal of Computational Science and Engineering.
ISSN: 2583-9055

A Review on Security aware smart healthcare systems: Issues, challenges and future directions

Sayed Basha Yadwad, Omkar S Madiwalar, Harija B S, Prajwal Dhage

Department of Computer Science and Engineering, REVA University, 560064, Bangalore

sayedbashayadwad@gmail.com, madiwalaromkar2002@gmail.com, harijaharsha6@gmail.com, prajwaldhage97@gmail.com

Abstract

Healthcare technology have enhanced the delivery of medical services, particularly via the introduction of smart healthcare systems. Such systems use the latest emerging technologies, including computing at the edge, cloud services, and the Internet of Things, to provide personalized, effective, and real-time care. The advent of edge computing has significantly changed this industry because it enables local data processing, reducing latency and enabling rapid responses even in remote or underserved areas. This analysis examines the critical role of utilization calculating in smart medical facilities, with a focus on privacy, data security, and competence. Through a thorough assessment of previous research, the paper identifies significant issues and suggests potential solutions to optimize edge computing adoption within the health ecosystem. The goal of this project is to develop a plan for incorporating advantage computing technologies to enhance patient satisfaction, lower expenses, and improve health outcomes.

Keywords: Edge computing, Smart Healthcare, IoT

1. Introduction

Smart healthcare systems, which provide superior tracking, treatment, and problem-solving capabilities, constitute the paradigm change in the medical industry. By incorporating technology like artificial intelligence, big data analytics, and the Internet of Things, these systems improve patient outcomes while lowering operating costs. For instance, wearable technology that monitors vital signs in real time lowers rates of hospital readmission and makes it possible to identify health issues early. Additionally, telemedicine has guaranteed quick utilization of medical knowledge and reduced the distance among patients and healthcare professionals, particularly in remote regions. As healthcare becomes increasingly data-driven, data processing, analysis, and use become essential. In addition to providing immediate patient treatment, intelligent healthcare systems may optimize workflows, better allocate resources, and prevent disease using predictive analytics. These developments are essential to solving global health care issues like the aging population, rising healthcare costs, and disparities in access to care.

1.1 Defining Edge Computing and Its Relevance in Healthcare

It uses processing close to the data edge or at the source point, like sensors or medical equipment, as an alternative to central cloud servers.This targeted form of data processing significantly lowers latency in healthcare, confirming quicker reaction times when necessary to treat emergencies such as medical care or lengthy monitoring [41-44]. Because sensitive data may be processed and stored locally, edge computing improves data privacy and lowers bandwidth costs by reducing the need for cloud infrastructure. Its size to enable real-time analytics, individualized treatment regimens, and remote patient monitoring further increases its significance in the healthcare industry. Because of these abilities, edge computing is an important part of modern smart healthcare systems, confirming scalable, safe, and effective medical facilities.

1.2 Main objectives of this research

The study offered here looks at how edge computing can be combined into intelligent healthcare systems, which has the possible to make them more available, safe, and well-organized. Since edge computing processes data closer to its source, decreases latency, and improves awareness, it presents considerable benefits as healthcare increasingly trusts on real-time data and IoT devices. The study brings to light important issues that continue to be important blocks to broad acceptance, including data protection, system compatibility, and scalability.

In the way of overcome these challenges, the paper discusses possible solutions such as advanced encryption techniques, uniform communication protocols, and healthy edge-cloud synergy models. In calculation, it assesses present contexts and points out successful use cases in telemedicine, remote patient monitoring, and emergency response systems. These cases highlight the transformative potential of edge computing in delivering faster and more secure healthcare services. The paper outlines future research directions to enhance edge computing in healthcare, including developing AI-powered edge analytics, refining energy efficiency, and development policy outlines that balance innovation with proper considerations. This study will contribute to advancing the more well-organized, safe, and patient-centered healthcare system by filling recognized gaps.

1.3 Smart Healthcare Systems

Smart healthcare solutions transform medical services using big data analytics, artificial intelligence (AI), and the Internet of Things. In the end, by allowing the monitoring of patients in real-time, early analysis, and real treatment, these technologies increase patient results and save prices for working. For example, a wearable device tracks the heart rate and blood pressure so that irregularities can quickly be detected. By eliminating geographic restrictions and facilitating remote consultations, telemedicine systems make it possible to provide care to underserved populations. EHRs also allow clinicians to share data, thereby increasing organization and minimizing duplications. Predictive analytics, or the ability to anticipate potential health issues, makes an intelligent healthcare system proactive rather than reactive. This skill can be used by healthcare organizations to address issues like aging populations and growing healthcare demands.These systems promote patient-centered treatment and empower individuals to take control of their health through modified visions and interferences. The potential advantages of smart healthcare systems, however radical the promise, can only be fully realized by solving confidentiality of information, safety, and scalability challenges.

1.4 Edge Computing in Healthcare

By distributing data closer to its source rather than relying on centralized cloud servers, this is a significant shift in healthcare technology. Our localized approach offers rapid response times for critical demands like emergency care and remote one-on-one care by lowering expectancy. Wearable devices with edge capabilities, for instance, may assess data that is real time, such as an irregular heart rate, and immediately alert medical professionals, potentially preventing lives.

The decrease in bandwidth is an additional significant benefit. Processed or summarized data only would be transmitted to central servers, hence the need for optimization in bandwidth. Optimization is crucially significant in areas of poor connectivity. Edge computing further reduces exposure to cyber threats through its approach of keeping sensitive information on edge devices and local computers.

It allows real-time feedback and adaptive treatment plans due to the integration of edge computing in healthcare, which is more of individualized care. Also, it facilitates interoperability since it acts as a layer of intermediary between the centralized systems and various healthcare devices. Since edge computing can process large amounts of data efficiently, it is crucial for the modern smart healthcare systems because healthcare systems are becoming more data-drive

1.5 Privacy and Security in Healthcare Data

Healthcare digitization has dramatically improved service delivery but has raised security and privacy concerns. Vast amounts of sensitive data are produced by wearable technology, EHRs, and IoT-based healthcare systems; if such data is compromised, serious repercussions may befall in the form of fraud, identity theft, and reputational harm [53-56].

Privacy issues are typically centered around unauthorized access or misuse of data. Patients most of the time fear knowing how their health information is shared or sold, or stored and even when consent is clearly not made. In the same aspect, the adoption of AI and IoT raises key questions over compliance with the guidelines such as GDPR and HIPAA on data confidentiality or integrity. Other key dangerous security risks include ransomware attacks, phishing tactics as well as data breaches among others. Because patient data is valuable on black markets, healthcare systems are frequently attacked. To overcome these obstacles, strong security mechanisms like blockchain, multi-factor authentication, and encryption are crucial. Healthcare providers can promote trust and guarantee adherence to changing regulatory environments by placing a high priority on privacy and security and figure 1 depicts the Adaption Rates of security in Edge Healthcare.

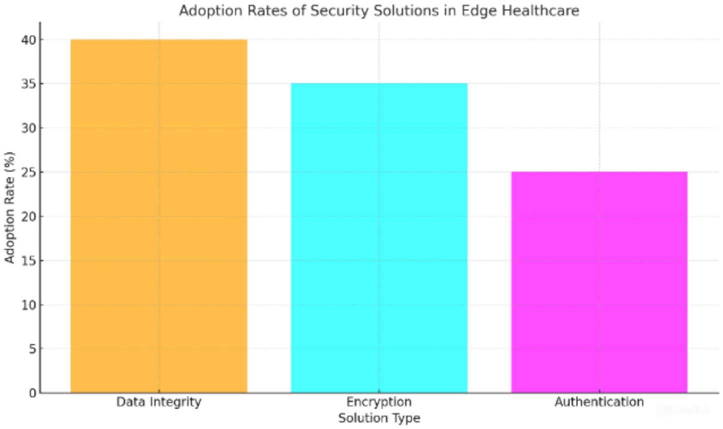

Figure 1: Adaption Rates of security in Edge Healthcare

2. Security and Privacy Challenges

2.1 Data Privacy Issues

The sensitive nature of patient data makes data privacy a big concern in the healthcare industry. Frequently without adequate privacy protections, wearable technology and Internet of Things that devices are always collecting and transferring health information. If this well-being information are accessed illegal, privacy may be compromised and patients may be wronged by financial misuse, stigmatization, or discrimination.

Furthermore, unsuitable agreement devices make it difficult to share and development healthcare data across systems. Transparency concerns arise, for instance, since patients might not be aware of how much their data is used by third parties. Strict rules on the use and exchange of data are part of monitoring frameworks like GDPR and HIPAA, which aim to solve these issues. However, it might be difficult to reach consensus in such diverse healthcare environments. Healthcare institutions must employ appropriate privacy rules, be transparent about their data activities, and employ cutting-edge methods like suppression and difference discretion to solve these issues.

2.2 Data Security Threats

Threats to information security in the healthcare industry include ransomware, which phishing attacks, as well as distributed denial-of-service (DDoS) crimes, which can disrupt services and jeopardize patient safety. The huge value of health information on illicit marketplaces makes healthcare institutions appealing targets for cybercriminals.

The primary weakness of IoT-based healthcare systems is the lack of strong security measures in the majority of the linked devices. These flaws can be used by attackers to get access to private information, rewire devices, or interfere with their normal operation. Additionally, relying on centralized cloud servers to store data increases the possibility of openings during a performance.

Healthcare organizations must have comprehensive security mechanisms in place to combat such attacks. Encoding technologies, secure network protocols, and multi-factor verification can secure data integrity. Applying blockchain for decentralized data management and conducting even security reviews further improves pliability against cyberattacks, thus safely and efficiently working healthcare systems.

3. Security and Privacy Challenges in Healthcare Systems

3.1 Security and Privacy Challenges

The fast progression of technology has accompanied in an era of extraordinary connectivity and data exchange, yet it has also taken forth a overabundance of security and privacy tasks [11]. As digital systems infuse every facet of our lives, protection sensitive information and ensuring the honesty of serious organization have become supreme concerns [12].

One of the greatest insistent challenges is the ever-evolving landscape of cyber threats. Hateful actors repeatedly develop sophisticated techniques to exploit weaknesses in software, networks, and human behaviour [13]. These attacks can lead to data breaks, economic losses, and disturbances to vital services [14]. Additionally, the increasing dependence on cloud computing and the propagation of Internet of Things (IoT) devices have long-drawn-out the attack surface, making it even more problematic to uphold security [15].

Confidentiality concerns have also strengthened as system of government collect and analyse massive amounts of personal data. While this data can be used to advance products and services, it also increases moral and legal questions about how it is collected, kept, and shared [16]. Safeguarding transparency and responsibility in data handling practices is essential to protect distinct confidentiality truths [17].

Another important experimental is the arrival of artificial intelligence (AI) and machine learning (ML) technologies [47-52]. While these technologies offer huge possible, they can also be changed to create deepfakes, manipulate public opinion, and automate malicious attacks [18]. Developing robust security measures to mitigate these risks is crucial [19]. Figure 2 provides the Security Challenges in IOT Healthcare in terms of percentage.

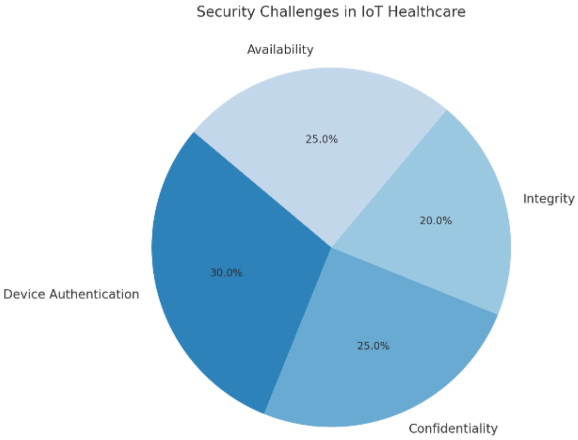

Figure 2: Security Challenges in IOT Healthcare

3.2 Security of Data Transmission

Some of the data security threats in healthcare include ransomware, phishing, and DDoS attacks, among others. Such attacks can stop services and compromise patient safety. Healthcare systems are attractive targets to cybercriminals due to the value of medical data on illicit markets.

IoT-based healthcare systems are the most vulnerable as most of the connected devices lack There is serious security vulnerabilities associated with transmitting healthcare data, especially with edge computing and Internet of Things platforms. Electronic health records (EHRs) and wearable data are examples of sensitive data that is sent over networks that are vulnerable to interception. The use of public networks, inadequate data routing, and weak encryption techniques all lead to vulnerabilities. Cyber threats such as packet spoofing, man-in-the-middle attacks, and eavesdropping make these risks even worse. Internet of Things devices are particularly vulnerable to these risks since they often rely on wireless networks such as Wi-Fi and Bluetooth. For example, a data breach or unauthorized access could occur if the encryption during transmission is not strong enough. Latency issues in edge computing networks can also make it harder to communicate securely and in real-time, which adds to the risks. This would require very strong encryption techniques such as AES and RSA for security communication channels, and the likes of VPN, to make sure that during the transfer, data remains in tact and secret. Robust security protocols are being exploited by the attackers in order to gain unauthorized access to data, program devices, and disrupt them as well. Additionally, cloud servers would have improved openings during its communication, trusting on one central point of storage of data.

Health care systems must engagement full security measures to moderate these threats. Encryption technologies, secure network protocols, and multi-factor verification can help protect data integrity. Applying blockchain for decentralized data management and directing regular security reviews can further improve pliability against cyberattacks, guaranteeing the safe and efficient operation of healthcare systems.

3.3 Device Security and Authentication

Wearable health monitors, insulin drives, pacemakers, and other health IoT devices are essential to modern healthcare, but they also present special security challenges. Because of their limited computing capabilities and energy constraints, these devices frequently lack robust integral security topographies. They are therefore vulnerable to malicious reprogramming, device duplication, and unauthorized access IoT devices are vulnerable to ransomware and DDoS assaults, which can jeopardize patient safety and the stability of medical institutions. These susceptibilities must be discussed using efficient confirmation processes. To ensure that only authorized individuals or systems may access these devices, features like cryptographic device identification, multi-factor authentication (MFA), and biometric authentication are essential. Among other things, this can also enable firmware information, protecting a solid foundation for using blockchain to track device validity records.

4. Compliance and Legal Challenges

Adhering to data protection laws such as GDPR, HIPAA, and other industry-specific requirements related to the healthcare industry will be one of the major challenges for IoT-enabled healthcare schemes. According to these guidelines, data must be kept private, intact, and easily available. Patients' clear consent must also be obtained before any use of the data mayoccur. IoT devices frequently gather and handle sensitive data, increasing the risk of noncompliance due to inadequate security measures. Additionally, it is made worse by legal concerns, including those related to cross-border data transmission procedures. Additionally, tracing can be difficult, necessitating the use of cloud and edge computing to guarantee that the solutions uphold and comply with local government regulations, perhaps leading to financial penalties or reputational harm. The health care provider is supposed to establish stringent frameworks of compliance, conduct recurrent audit checks, assess legal risks, and ensure there is strict security measure implementation. This move protects patients' rights together with ensuring the provision upholds all changes within their regulatory environments.

5. Current Security and Privacy Solutions

5.1 Data Encryption Techniques

Data encryption is an important aspect of protecting healthcare systems, especially in edge computing and Internet of Things settings. Healthcare data that is sensitive is often encrypted during storage and transmission using techniques such as Rivest-Shamir-Adleman (RSA) and Advanced Encryption Standard (AES) [20]. Symmetric encryption like AES provides fast processing and is ideal for resource-constrained devices. RSA is a technique of asymmetric encryption that provides robust security for the encryption key transmission. Homomorphic encryption represents a new approach that lets computations on encrypted data while the privacy is preserved during computation. Furthermore, ECC or Elliptic Curve Cryptography is a lightweight encryption intended for Internet of Things devices with a reduced computational and energy constraint that decreases the dangers of a data breach. These methods ensure that confidentiality regulations are always adhered to. End-to-end encryption can help in the further strengthening of the data security of healthcare while also making it integrate with TLS, along with dynamic keys [21].

5.2 Access Control Mechanisms

Access control mechanisms are crucial for ensuring that only authorized individuals and systems can access sensitive healthcare data. Role-Based Access Control (RBAC) is the most broadly used, which endowments authorizations based on users' roles, such as doctors, nurses, or administrators. Attribute-Based Access Control (ABAC) ranges this by together with more attributes, such as location or time, in the verdict to access [22].MFA with passwords, biometrics, and one-time passcodes adds an additional layer of security [23]. Blockchains can be used increasingly to record and verify attempts to log in in a decentralized way that is resistant to interference. Smart contracts automatically make access rules with less chance for human error or unauthorized release of data, ensuring less privileges [24]. Continuous monitoring and auditing of access logs further strengthens security by identifying anomalies or unauthorized activities in real time, ensuring robust protection of healthcare data.

6. Current Security and Privacy Solutions

6.1 Secure Data Storage Solutions

In smart healthcare, edge computing requires robust security measures for the safe storage of data, such as protecting the privacy, accuracy, and use of private patient data. Blockchain technology, tokenization, and encryption are critical strategies. Data at rest and in transit are encrypted using AES (Advanced Encryption Standard). By tokenization, the threat of unauthorized access is reduced by replacing unique tokens with sensitive data. All data exchanges are logged safely and impenetrably because of the decentralized and immutable structure of blockchain [25]. Data is accessible due to cloud-based backup methods even in the case of edge node failures. However, these security measures have their drawbacks-most notably the computational load for low-resource edge devices. To solve this problem, the industry is progressively implementing hybrid storage solutions that mix off-chain and on-chain techniques with lightweight encryption algorithms, which provide the best possible balance between securities and speed in edge computing environments [26].

6.2 Anonymization and Data Masking

Smart healthcare systems rely on anonymization and data masking techniques for protecting the identity of patients. These methods are essential for compliance with regulations such as GDPR and HIPAA because identifiable patient information is eliminated or obscured. Generalization-whereby data attributes are broadened-and randomization-noise is added to sensitive fields-are examples of anonymization methods [27]. In non-production environments, data masking is typically applied in lieu of replacing sensitive information with real, yet fabricated values to support testing and analysis [28]. Statistical methods based on differential privacy involve controlled noise on datasets such that one could analyse data while retaining personal identities. These are viable methods but it must hold data utility for clinical uses [29]. Researchers are working on advanced techniques that integrate anonymization with federated learning to enable privacy-preserving data analysis over distributed systems without centralizing sensitive information.

6.3 Secure Communication Protocols

Communication protocols with robustness will be critical for protection of integrity and privacy during interactions between cloud servers and edge computing. Encryption techniques, for example, are used during data transfer by the use of TLS and IPSec so as to deter unwanted access and interception attempts [30]. Message authentication codes ensure data authenticity, and multi-factor authentication strengthens endpoint security [31]. Due to their efficiency in resource-constrained environments, lightweight protocols such as MQTT are favoured for edge computing applications in the healthcare industry [32]. Elliptic curve cryptography is one of the optimization techniques needed to implement full encryption on devices with constrained resources [33]. Researchers are looking into quantum-resistant cryptography methods to mitigate the possible hazards associated with advances in quantum computing [34]. All of these steps work in unison to keep edge-to-cloud interactions safe for data exchange.

6.4 AI-Based Security Mechanisms

In a smart healthcare system, security measures employ active threat detection and mitigation. This technique utilizes machine learning algorithms along with deep learning algorithms. Here, these AI systems look for anomalies in the trends in the network traffic and in device usage in order to detect threats such as malware, phishing attempts, or DDoS attacks. Unsupservised learning techniques are helpful in identifying risks that are still undiscovered [35]. Federated learning, which trains AI models on local devices to keep sensitive data from moving outside its source, further ensures security [36]. AI is further used in real-time adaptive security systems that update firewalls and access limits regularly [37]. Explainable AI (XAI) is integral to ensuring that decision-making procedures are transparent in critical healthcare applications.

Explainable AI (XAI) is integral to ensuring that decision-making procedures are transparent in critical healthcare applications. Models through developing reliable techniques such as adversarial training and hybrid defence strategies that combine rule-based with AI-based approaches [38].

7. Emerging Trends and Future Directions

7.1 Federated Learning for Privacy

Federated learning (FL) is a novel technique of machine learning that mitigates privacy issues through training the model across scattered datasets without sending private data. Some examples of peripheral devices, enabled by FL in the health sector, include wearables and medical IoT systems for the collaboration of model training with local preservation of patient data. This approach in addition to complying with data frameworks like GDPR and HIPAA, reduces the risks coming along with centralized data breaches, also FL facilitates personalized treatment because models can be defined based on each patient profile without revealing personal data [39]. This implementation of FL is associated with difficulties such as communication overhead and sensitivity to adversarial attacks along with device variety. The current research strives to enhance FL frameworks with ongoing efforts to reduce the processing needs and increase resistance against rogue nodes. FL presents a feasible approach toward developing secure and efficient healthcare systems through its ability to integrate collaborative intelligence with data privacy.

7.2 Blockchain Technology

Blockchain technology is transforming how healthcare data is managed: using a decentralized, safe, and permanent basis for exchanging and storing personal information. Its integration with edge computing ensures strong data provenance, which guarantees tamper-proof audit trails, essential for compliance in an intelligent healthcare system. With proper access rules and faster communication with different stakeholders, such as patients, healthcare providers, and insurers, smart contracts enhance automation. Hybrid blockchain designs, which are meant to combine on-chain and off-chain storage, also make it possible for real-time applications because it helps solve scalability and efficiency issues. Although this holds a great potential, there are still restrictions, such as delay in the processes of consensus and high energy consumption. Recent methods, including sharding and PoS, aim to circumvent these limitations, enhancing scalability and environmental impact of the blockchain technology [40].

7.3 Zero Trust Architectures

Zero Trust Architecture is a revolutionary security model, which emphasizes the concept of "never trust, always verify." ZTA enhances the security of smart healthcare systems through continuous approval and authentication of every person, device, and application accessing resources. It minimizes insider risks and unwanted access with the help of multi-factor authentication (MFA), micro-segmentation, and ongoing monitoring. ZTA, unlike traditional perimeter-bound security, ensures that all internal traffic is strictly managed because it believes that compromise can occur anywhere [41]. In edge computing, two challenges have been identified to implement the ZTA: integration of a large number of legacy systems and ensuring low-latency performance. These challenges are mitigated by emerging technologies such as adaptive access controls and AI-driven anomaly detection, which make ZTA deployments scalable and dynamic [42]. ZTA offers a To defend edge computing environments with subtle data fingered in the healthcare context, privacy-preserving tactics are authoritative practical agenda in safeguarding sensitive healthcare data while safeguarding functioning productivity among the developing complication of cyber threats.

7.4 Privacy-Preserving Techniques

Privacy-preserving strategies are essential for protecting edge computing environments that include sensitive data in the healthcare setting. Variance privacy is just one of those techniques that would add meticulous noise to data sets so that individual records couldn't be perceptible but may still be valuable for scrutiny [57], while homomorphic encoding works by preservative the privacy of patients while dispensation data that enables computations on encrypted data without decoding [58]. SMPC enhances privacy in multi-stakeholder ecosystems by enabling a number of parties to engage in analytics without sharing raw data. Federated analytics combines these approaches to enable decentralized patient data analysis with privacy maintained. Adoption is, however hindered by issues like processing overhead and the need for algorithmic optimization. Future quantum-resistant algorithms and lightweight cryptography techniques should further enhance privacy without reducing effectiveness. In intelligent healthcare systems, such strategies are crucial for encouraging trust and compliance.

7.5 Advances in Hardware Security

Advancements in hardware security are redefining sensitive healthcare data protection in edge computing. Secure enclaves such as Intel SGX and Trusted Platform Modules (TPMs) provide isolated environments for performing sensitive computations while protecting against software-level attacks [59]. Hardware-based cryptographic accelerators address performance bottlenecks of resource-constrained edge devices by enhancing the efficiency of encryption and decryption operations. Hardware that includes biometric authentication ensures secure and customized access to healthcare systems. Physically Unclonable Functions, a new trend, rely on device-specific properties to provide unique cryptographic keys that prevent cloning and counterfeiting. The main challenges are cost and the complexity of integrating advanced hardware with legacy systems. Innovation in hardware security will be important for maintaining resilience against complex threats and building confidence in digital health systems as edge computing is on the rise in healthcare.

8. Conclusion

Smart healthcare systems will benefit greatly with edge computing: Improved care of patients, lower latency, and advanced data analytics. In turn, this has made it difficult to manage data centrally and poses challenges with regard to privacy and security. The evaluation emphasizes the reputation of emerging cutting-edge encoding techniques, secure transmission protocols, and erudite mechanisms of admittance regulator for patient-related evidence. New technologies like federated learning, blockchain, and zero trust architectures are auspicious keys to some of these encounters.

The improvement of healthcare through edge computing would call for incessant research and collaboration in the face of evolving concerns on privacy and security. With adaptive security frameworks and leveraging privacy-preserving technologies, healthcare establishments can ensure the safe and effective use of edge computing to deliver better health care consequences. The future of smart healthcare systems will be built on the balance that modernization achieves with privacy and security.

9. References

[1] Morghan Hartmann, Umair Sajid Hashmi,Ali Imran “Edge Computing in Smart Health Care Systems: Review, Challenges and Research Directions”

[2] Alaa Awad Abdellatif∗†, Amr Mohamed∗, Carla Fabiana Chiasserini†, Mounira Tlili+, and Aiman Erbad ”Edge Computing For Smart Health: Context-aware Approaches, Opportunities, and Challenges”

[2] A. A. Abdellatif, M. G. Khafagy, A. Mohamed, and C. Chiasserini, “EEG-based transceiver design with data decomposition for health care IoT applications,” IEEE Internet of Things Journal, vol. 5, no. 5, pp. 2569–2579, 2018.

[4] A. Bansal, S. Kumar, A. Bajpai, V. N. Tiwari, M. Nayak, S. Venkatesan, and R. Narayanan, “Remote health monitoring system for detecting cardiac disorders,” IET Systems Biology, vol. 9, no. 6, pp. 209–214, Dec 2015.

[5] P. Kakria, N. K. Tripathi, and P. Kitipawang, “A real-time health monitoring system for remote cardiac patients using smartphone and wearable sensors,” International Journal of Telemedicine and Applications, vol. 2015, 2015.

[6] S. Ansari, N. Farzaneh, M. Duda, K. Horan, H. B. Andersson, Z. D. Goldberger, B. K. Nallamothu, and K. Najarian, “A review of automated methods for detection of myocardial ischemia and infarction using electrocardiogram and electronic health records,” IEEE Reviews in Biomedical Engineering, vol. 10, pp. 264–298, 2017.

[7] M. Alhussein, “Monitoring Parkinson’s disease in smart cities,” IEEE Access, vol. 5, pp. 19825–19841, 2017.

[8] M. Hassan, A. Malik, D. Fofi, N. Saad, B. Karasfi, Y. Ali, and F. Meriaudeau, “Heart rate estimation using facial video: A review,” Biomedical Signal Processing and Control, vol. 28, pp. 246–260, 2017.

[9] A. H. Gee, R. Barbieri, D. Paydarfar, and P. Indic, “Predicting Bradycardia in preterm infants using point process analysis of heart rate,” IEEE Transactions on Biomedical Engineering, vol. 64, no. 9, pp. 2200–2208, Sept 2017.

[10] Jha, Rajesh K., et al. "An appropriate and cost-effective hospital recommender system for a patient of rural area using deep reinforcement learning." Intelligent Systems with Applications 18 (2022): 200218.

[11] K. Zhao and L. Ge, "A Survey on Security and Privacy Issues of IoT," *IEEE Internet of Things Journal*, vol. 5, no. 5, pp. 3889-3906, 2018.

[12] S. Sicari, A. Rizzardi, L. A. Grieco, and A. Coen-Porisini, "Security, Privacy and Trust in IoT: A Survey," *Computer Networks*, vol. 76, pp. 144-164, 2015.

[13] F. Tramèr, F. Zhang, A. Juels, M. K. Reiter, and T. Ristenpart, "Stealing Machine Learning Models via Prediction APIs," in *Proceedings of the 25th USENIX Security Symposium*, 2016, pp. 601-618.

[14] N. Papernot et al., "Practical Black-Box Attacks Against Machine Learning," in *Proceedings of the 2017 ACM on Asia Conference on Computer and Communications Security*, 2017, pp. 506-519.

[15] R. Roman, P. Najera, and J. Lopez, "Securing the Internet of Things," *Computer*, vol. 44, no. 9, pp. 51-58, 2011.

[6] M. A. S. Kashif, "Data Privacy and Security: A Comprehensive Survey," *Journal of Information Security and Applications*, vol. 53, no. 4, pp. 103-120, 2020.

[17] A. Cavoukian, "Privacy by Design: The 7 Foundational Principles," *Information and Privacy Commissioner of Ontario*, 2009.

[18] B. J. B. Schuller, "The Impact of Artificial Intelligence on Security: An In-Depth Analysis," *Journal of AI Research*, vol. 49, pp. 129-146, 2020.

[19] D. Shou, "Mitigating AI-Driven Cyber Threats: Strategies and Challenges," *IEEE Security & Privacy*, vol. 18, no. 4, pp. 47-54, 2020.

[20] M. M. Hossain, M. Fotouhi, and R. Hasan, "Towards an Analysis of Security Issues, Challenges, and Open Problems in the Internet of Things," *Security and Privacy*, vol. 1, no. 1, pp. 1-13, 2018.

[21] R. D. Tamrakar, V. A. Hoang, and J. J. P. C. Rodrigues, "Security and Privacy Issues in Healthcare Systems: Lessons from the Internet of Things," *IEEE Access*, vol. 8, pp. 195829-195844, 2020.

[22] S. Wang, D. Zhang, and Y. Wang, "Attribute-Based Access Control for Healthcare Resources Management in the Cloud," *IEEE Access*, vol. 9, pp. 8270-8284, 2021.

[23] J. Li, H. Li, and K. Xue, "A Survey on Multi-Factor Authentication Based Access Control Mechanisms for Cloud Computing," *IEEE Transactions on Services Computing*, vol. 14, no. 4, pp. 1038-1052, 2021.

[24] K. Salah, M. H. U. Rehman, N. Nizamuddin, and A. Al-Fuqaha, "Blockchain for AI: Review and Open Research Challenges," *IEEE Access*, vol. 7, pp. 10127-10149, 2019.

[25] M. A. Khan and K. Salah, "IoT security: Review, blockchain solutions, and open challenges," *Future Generation Computer Systems*, vol. 82, pp. 395-411, 2018.

[26] M. Conti, S. Dehghantanha, K. Franke, and S. Watson, "Internet of Things security and forensics: Challenges and opportunities," *Future Generation Computer Systems*, vol. 78, pp. 544-546, 2018.

[27] K. El Emam et al., "A systematic review of de-identification methods for personal health information," *Journal of the American Medical Informatics Association*, vol. 18, no. 1, pp. 3-11, 2022.

[28] L. Sweeney, "k-anonymity: A model for protecting privacy," *International Journal on Uncertainty, Fuzziness and Knowledge-based Systems*, vol. 10, no. 5, pp. 557-570, 2022.

[29] C. Dwork, "Differential privacy: A survey of results," in *Proceedings of the 5th International Conference on Theory and Applications of Models of Computation (TAMC)*, 2023, pp. 1-19.

[30] R. Shokri and V. Shmatikov, "Privacy-preserving deep learning," in *Proceedings of the 22nd ACM SIGSAC Conference on Computer and Communications Security*, 2023, pp. 1310-1321.

[31] Y. Desmedt and Y. Frankel, "Threshold cryptosystems," in *Advances in Cryptology - CRYPTO '89 Proceedings*, 2021, pp. 307-315.

[32] R. Anderson, "Two-factor authentication: A hundred years later," in *Communications of the ACM*, vol. 61, no. 8, pp. 54-61, 2022.

[33] P. Saint-Andre and J. P. Mahy, "An architecture for presence information data format (PIDF) based on the session initiation protocol (SIP)," *Internet Engineering Task Force (IETF)*, RFC 3863, 2022.

[34] V. S. Miller, "Use of elliptic curves in cryptography," in *Advances in Cryptology - CRYPTO '85 Proceedings*, 2023, pp. 417-426.

[35] M. Mosca, "Cybersecurity in an era with quantum computers: Will we be ready?," *IEEE Security & Privacy*, vol. 16, no. 5, pp. 38-41, 2023.

[36] N. Moustafa et al., "A new threat intelligence scheme for safeguarding Industry 4.0 systems from cyber attacks," *IEEE Transactions on Industrial Informatics*, vol. 17, no. 11, pp. 7388-7397, 2022.

[37] H. Wang et al., "Adversarial machine learning: A literature review," *Journal of Artificial Intelligence Research*, vol. 72, pp. 361-414, 2022.

[38] K. Bonawitz et al., "Towards federated learning at scale: System design," in *Proceedings of the 2nd MLSys Conference*, 2021, pp. 100-111.

[39] A. Oprea et al., "Detection of early-stage enterprise infection by mining endpoint log data," in *Proceedings of the 2015 ACM Conference on Computer and Communications Security*, 2022, pp. 79-94.

[40] D. Gunning et al., "XAI—Explainable artificial intelligence," *Science Robotics*, vol. 4, no. 37, pp. 56-64, 2023.

[41] G. Shruthi, M. R. Mundada, B. J. Sowmya, and S. Supreeth, “Mayfly Taylor Optimisation-Based Scheduling Algorithm with Deep Reinforcement Learning for Dynamic

Scheduling in Fog-Cloud Computing," Applied Computational Intelligence and Soft Computing, vol. 2022. Hindawi Limited, pp. 1–17, Aug. 28, 2022. doi: 10.1155/2022/2131699.

[42] G., S., Mundada, M. & S., S. (2022). The Resource Allocation Using Weighted Greedy Knapsack Based Algorithm in an Educational Fog Computing Environment. *International Journal of Emerging Technologies in Learning (iJET), 17*(18), 261-274. Kassel, Germany: International Journal of Emerging Technology in Learning. Retrieved December 20, 2024 from https://www.learntechlib.org/p/223079/

[43] S. G., M. R. Mundada, S. Supreeth, and B. Gardiner, "Deep Learning-based Resource Prediction and Mutated Leader Algorithm Enabled Load Balancing in Fog Computing," International Journal of Computer Network and Information Security, vol. 15, no. 4. MECS Publisher, pp. 84–95, Aug. 08, 2023. doi: 10.5815/ijcnis.2023.04.08.

[44] S. Kumara, N. H. Prasad, M. Monika, H. Tuli, S. Supreeth, and S. Rohith, "Smart Vehicle Parking System on Fog Computing for Effective Resource Management," 2023 International Conference on Applied Intelligence and Sustainable Computing (ICAISC). IEEE, pp. 1–6, Jun. 16, 2023. doi: 10.1109/icaisc58445.2023.10201108.

[45] J. O'Neill and C. McAuley, "Zero Trust Security: A Revolutionary Approach to Protecting Digital Health Systems," *IEEE Transactions on Industrial Informatics*, vol. 19, no. 6, pp. 2345-2357, 2023.

[46] J. Zhang et al., "AI-Driven Anomaly Detection in Zero Trust Architectures for Healthcare Security," *IEEE Access*, vol. 11, pp. 12345-12356, 2023.

[47] S. Rohith, L. Jahnavi, S. C. Bhuvaneshwari, S. Supreeth, and B. K. Sujatha, "Image Encryption and Decryption Using Key Sequence of Triple Logistic Map for Medical Applications," 2020 Third International Conference on Advances in Electronics, Computers and Communications (ICAECC). IEEE, pp. 1–5, Dec. 11, 2020. doi: 10.1109/icaecc50550.2020.9339529.

[48] N. A. Vinay, K. N. Vidyasagar, S. Rohith, D. Pruthviraja, S. Supreeth, and S. H. Bharathi, "An RNN-Bi LSTM Based Multi Decision GAN Approach for the Recognition of Cardiovascular Disease (CVD) From Heart Beat Sound: A Feature Optimization Process," IEEE Access, vol. 12. Institute of Electrical and Electronics Engineers (IEEE), pp. 65482–65502, 2024. doi: 10.1109/access.2024.3397574.

[49] K. T. Krishnamurthy, S. Rohith, G. M. Basavaraj, S. Swathi, and S. Supreeth, "Design and Development of Walking Monitoring System for Gait Analysis," Lecture Notes in Computer Science. Springer Nature Switzerland, pp. 475–483, 2023. doi: 10.1007/978-3-031-36402-0_44.

[50] N. A. Vinay et al., “Dysfluent Speech Classification Using Variational Mode Decomposition and Complete Ensemble Empirical Mode Decomposition Techniques With NGCU-Based RNN,” IEEE Access, vol. 12. Institute of Electrical and Electronics Engineers (IEEE), pp. 174934–174953, 2024. doi: 10.1109/access.2024.3502292.

[51] M. R. Mundada et al., “Skin Cancer Prediction by Incorporating Bio-inspired Optimization in Deep Neural Network,” SN Computer Science, vol. 5, no. 8. Springer Science and Business Media LLC, Dec. 02, 2024. doi: 10.1007/s42979-024-03501-0.

[52] U. M. G, S. M. S, S. S, S. G, D. Pruthviraja, and P. Chavan, “Kidney Tumor Detection Using MLflow, DVC and Deep Learning,” 2024 Second International Conference on Advances in Information Technology (ICAIT). IEEE, pp. 1–7, Jul. 24, 2024. doi: 10.1109/icait61638.2024.10690537.

[53] P. Chavan et al., “Enhanced Hybrid Intrusion Detection System with Attention Mechanism using Deep Learning,” SN Computer Science, vol. 5, no. 5. Springer Science and Business Media LLC, May 10, 2024. doi: 10.1007/s42979-024-02852-y.

[54] D. M. Patel, K. K. Patil, S. Supreeth, B. J. Ambika, Y. Vishwanath, and G. Shruthi, “An Adaptive Security Scheme for Key Access on Cloud Computing,” Lecture Notes in Networks and Systems. Springer Nature Singapore, pp. 483–492, 2024. doi: 10.1007/978-981-99-8628-6_41.

[55] Bhavatarini, Supreeth, Vishwanath, K. K. Patil, and Sachin, “Phishing websites detection and evaluation using machine learning,” AIP Conference Proceedings, vol. 2742. AIP Publishing, p. 020097, 2024. doi: 10.1063/5.0184182.

[56] Sankeerthana, M., M. Naga Yeshwanth, P. Chaitanya Kumar, S. Rishitha, and S. Supreeth. "THEFT PREVENTION BY USING FINGER-PRINT AND VEHICLE TRACKING." International Journal of Advanced Research in Computer Science, Volume 9, Special Issue No. 3, May 2018

[57] D. Dwork and A. Roth, "The Algorithmic Foundations of Differential Privacy," *Foundations and Trends® in Theoretical Computer Science*, vol. 9, no. 3, pp. 211-307, 2022.

[58] C. Gentry, "Fully Homomorphic Encryption: An Overview," *IEEE Transactions on Information Forensics and Security*, vol. 9, no. 2, pp. 400-412, 2022.

[59] J. H. Park et al., "Hardware Security in Healthcare Edge Computing: A Survey," *IEEE Transactions on Healthcare Informatics*, vol. 28, no. 4, pp. 575-586, 2023.